# Password Standard

Effective: October 21, 2003
Revised: October 14, 2003
Owner: Michael Allred

## Purpose

The purpose of this policy is to establish a standard for the creation of strong passwords, the protection of those passwords, the frequency of change, and their timely removal.

## Scope

The scope of this policy includes all personnel who have access to State of Utah information resources with user ID and password authentication. All user IDs created on any State computing system or device should have an associated password that meets the standards of this policy.

## Background

This policy establishes a standard method for the creation, maintenance, and protection of passwords to be used by State agencies to protect the integrity and security of information systems. Agencies should use this general policy to develop their own specific password policies and procedures.

User IDs and passwords protect the integrity of information, provide authentication, control access, and establish user audit capabilities within the State of Utah computing environment and information resources. The combination of a user ID and password provide individual user validation that the person is authorized to access the system or device. Any individual accessing a State of Utah information resource, including employees, contractors, and vendors, is responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

## Policy

General Password StandardsAll supervisor-level passwords (e.g., root, enable, NT administration, and privileged accounts) should be changed on a regular basis, or, at minimum, every 45 days, or, when someone with administrative privileges, or a possible knowledge of those passwords, leaves the organization, or is no longer performing duties that require supervisor-level permissions.

- When possible, all user level passwords should be changed at least every 90 days.
- A history of a user's 10 most recently established passwords should be maintained to restrict their reuse.
- Inactive user accounts should be revoked after 90 days.
- Employees no longer employed or on contract must be removed from all systems and their user ID and password changed, revoked, or eliminated.
- After three consecutive unsuccessful password attempts a user ID should be revoked or disabled until reinstated or removed by the agency security administrator.
- Screen savers with passwords should be used on all computers (servers, laptops, workstations) and activated after no more than 15 minutes of inactivity.
- Employees should password lock their screens when leaving workstations unattended.
- All user accounts that have system-level privileges granted through group memberships should use passwords that are unique from all other accounts held by that user.

### General Password Construction Guidelines

All passwords should conform to the guidelines as described in this section.

User ID and password combinations are used for various purposes on State of Utah information systems and resources. Some of the more common uses include host, application, and network service access. Everyone using these information systems should be aware of how to select a strong password. Strong passwords have the

following characteristics:

- A password should be at least eight alphanumeric characters long.
- A password should not be a word in any language, slang, dialect, jargon, etc.
- When possible, passwords should have a combination of numeric digits and special characters, as well as lower and upper case letters.
- Passwords should include three of the following four attributes:
    - One Upper Case Character
    - One Lower Case Character
    - One Numeric Character
    - One Special Character
- Passwords should not be based on personal information, names of family members, pets, etc.
- When changing a password it is not acceptable to simply add a number to the end of the previous used password. For example password1, password2, etc.

**Password Creation Suggestions**

Users should try to create passwords that can be easily remembered but not easily guessed. One way to do this is to create a password based on a song title, affirmation, or other phrase.

***Examples of ways to create passwords:***

- "I am going to a party for him." The password could be: "IAG2AP4H"
- "This may be one way to remember." The password could be: "TmB1W2R"
- "At work I am on my best behavior." The password could be: "wIaombb"
- "Money is a good asset to have." The password could be: "$isaga2h"
- "The number 7 is a lucky number." The password could be: "T#7isal#"

**Password Protection Standards**

- Passwords should never be sent in clear text over the network. This includes e-mail, chat, instant messaging, or any other non-secure form of information transfer.

- Passwords should never be stored in unsecured places, such as written down on a sticky note or saved unprotected on-line.

- Passwords used for the State of Utah computing environment and information resources should be different than those used for personal accounts (e.g., a personal ISP account, option trading, benefits, etc.).

- User IDs and passwords should never be shared with anyone, including administrative assistants, coworkers, family members, a local network administrator, your boss, or secretaries.

- All passwords should be treated as sensitive, confidential State of Utah information.

- Security and network administrators should never ask you to divulge your password.

**Protocol or Application Specific Passwords**

Whenever installing new software or applications, always change the default password as soon as possible.

Where SNMP is used, the community strings should be defined as something other than the standard defaults of “public,” “private,” and “system,” and should be different from the passwords used to log in interactively. A keyed hash must be used where available (e.g., SNMPv2).

A user ID with total system privileges should not be used to perform backup. Backup user IDs often have read and write privileges to entire systems. Extra care should be taken to prevent possible comprise of this type of user ID and password. The strongest possible password should be used and changed on a regular basis for the backup user ID.

**If a Password or User ID is Compromised**

At any time a user ID or password is suspected of being compromised, the password should be changed immediately, or the account disabled.